Rick Hance

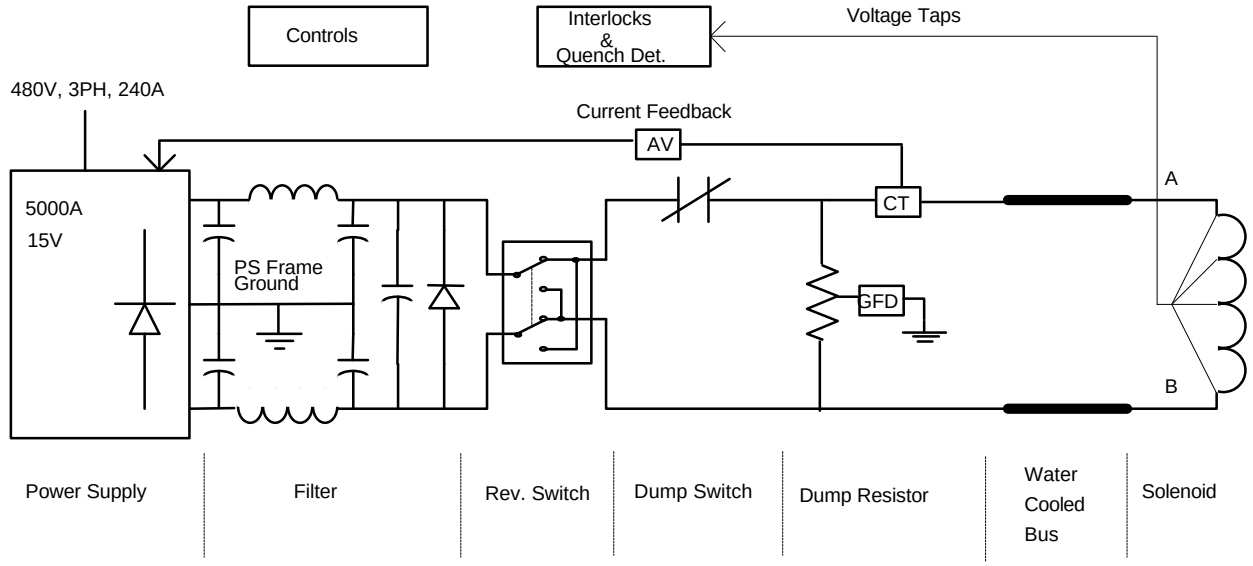
Engineering Note

Date: 12/03/97
Rev Date: 01/21/98

Project: Solenoid Energization, Control, Interlocks and Quench Protection
Doc. No: H971203B

Subject: Solenoid Quench Protection System Single Device Failure Analysis

This document has been prepared in anticipation of conducting power tests on the DZERO Central Tracking Solenoid energization system. In particular, we will review the critical functions of the Quench Protection System. It was noted by the Electrical Safety Committee after their preliminary safety review, that the mechanism of sensing a quench, lead failures, and turning off the power supply should have redundant paths to ensure that no single device failure could result in damage to the superconducting solenoid or its chimney leads. This document will discuss the relevant issues and describe the mechanisms that provide this redundancy. This document is intended for an audience already familiar with the system being discussed[1]. No overview will be given here except for the general diagram shown below for reference.



Critical Functions of the Quench Protection System -- The technical specification for the solenoid requires that it "shall not sustain damage of any kind (i.e. be self-protecting) when quenched from design operating current or any fraction thereof" with or without an external protection resistor[2]. Conformance to the specification has been proven in testing[3]. This information is presented in order to establish the understanding that the quench protection system is not absolutely required to remove the stored energy from the solenoid after a quench. However, the solenoid and its superconducting leads are not specified to absorb additional energy from the

[1] The Solenoid Energization, Controls, Interlocks and Quench Protection system is described in D0 Engineering Note 3823-111-EN-418 and other documents available at http://d0sgi0.fnal.gov/~hance/solenoid

[2] Section 5.4.3 through 5.4.6 of the Technical Specification for a 2 Tesla Superconducting Solenoid Magnet for D0 at Fermilab. Specification number E823-94-01 Rev 8 1/1/94.

[3] Approval letter FTF-131 Smith (Fermilab) to Kozu (Toshiba) dated 4/16/97.

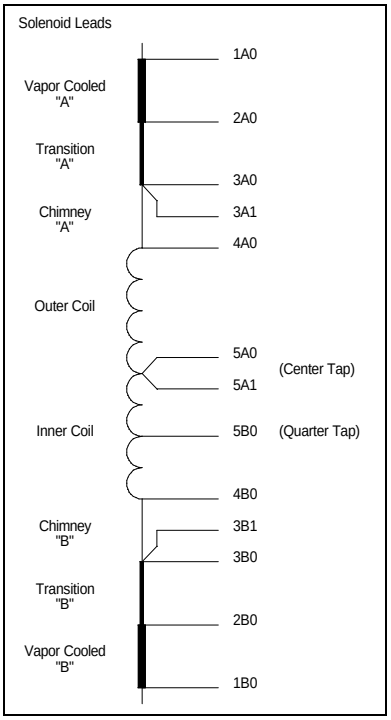
power supply after a quench i.e. the power supply must be disabled if a quench occurs. Additional energy from the power supply after a quench could have the following adverse effects:

1. Resistance heating in the solenoid requiring additional cool-down time to return to superconductivity after a quench.
2. Possible over-current damage to the vapor cooled, transition, and chimney leads if the solenoid coil were to remain superconducting after the leads have become resistive. The windings of the solenoid coil itself have sufficient resistance to limit the maximum current in the coil from the 15V power supply to safe levels (15V/1.58Ω=9.49A)[4]. The leads alone however, do not have this inherent current limiting.

Thus, the "critical" function of the quench protection system is to detect the occurrence of a quench either in the solenoid or its superconducting leads; and to turn-off the solenoid power supply or disconnect it from the solenoid and dump resistor by opening the dump switch. Either way, the power supply must be disabled from continuing to deliver energy to the solenoid.

The function of the dump switch is to facilitate the external dissipation of the energy stored in the solenoid, thus decreasing the discharge time and reducing the load on the solenoid cooling system. When the dump switch opens, the filter and power supply bypass diodes are removed from the circuit and the solenoid energy is mostly dissipated in the dump resistor. The dump resistor is a discreet device, conservatively designed from stainless steel bar stock with no moving parts[5]. It is permanently attached across the solenoid; and thus has no likely failure mode. Since the solenoid can absorb its own energy, the operation of the dump switch is not considered critical to the quench protection of the solenoid except in the case of a failure to turn off the power supply. Likewise, the turning off of the power supply is not considered critical to quench protection except in the case of a failure to open the dump switch. By opening the dump switch, the power supply is removed from the circuit whereupon it merely idles with no load.

Mechanism of sensing a quench – Quenches are detected by hardware circuits that monitor voltage taps strategically located on the solenoid and its leads and buses[6]. Superconducting chimney buses will have essentially zero voltage across them during charging, discharging and steady state operation. These voltages are monitored directly. Vapor cooled leads will develop some voltage depending on the current flowing through them. These voltages are compensated for current during signal processing. The solenoid coil will develop voltage across it during charging & discharging. This voltage is accounted for by using bridge circuits that compare 1/2 and 1/4 of the solenoid voltage with respect to its center and quarter taps respectively. The voltage taps from the solenoid apparatus are illustrated below.



The voltage taps are brought out of the solenoid to resistor/test point boxes located within inches of the solenoid and control dewar ports. In the resistor/test point box, the voltage taps are grouped as required to accommodate quench detection; and each signal of each group is individually isolated with a 10K resistor.

The voltage tap groups are as follows:

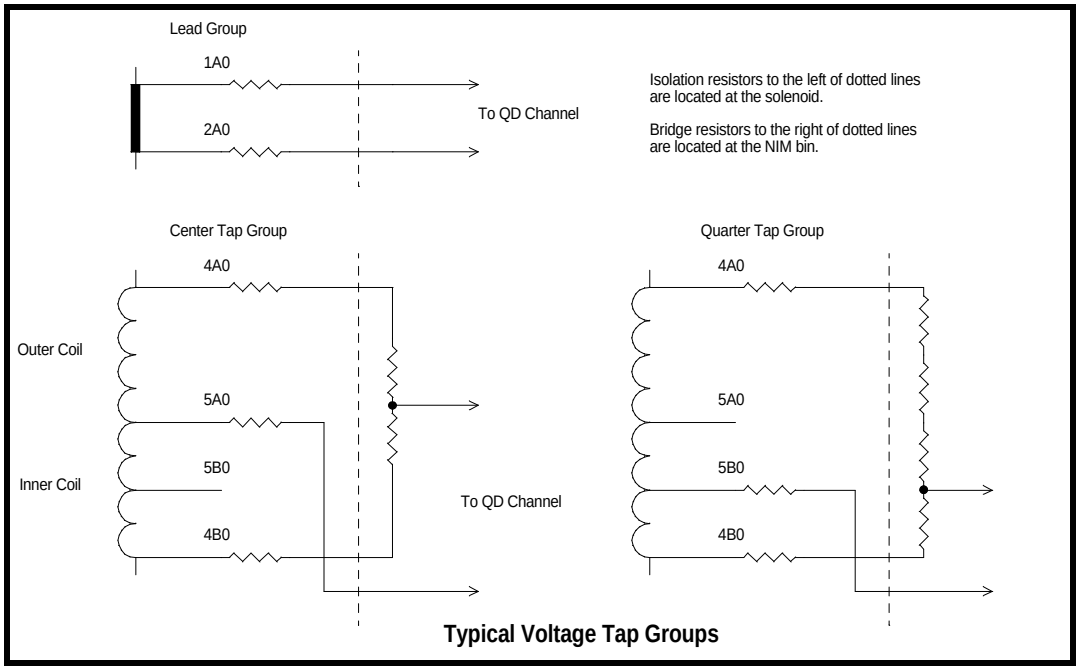
- Differential voltage across each vapor cooled lead (A & B).
- Differential voltage across each transition lead (A & B).
- Differential voltage across each chimney lead (A & B).
- Center tap and outside buses of coil – to be used to compare the center tap voltage to the 1/2 point of a bridge derived across the outside of the coil.
- Quarter tap and outside buses of coil – to be used to compare the quarter tap voltage to the 1/4 point of a bridge derived across the outside of the coil.

[4] D0 Engineering Note 3823.111-EN-374 Energy Losses in the D0 β Solenoid Cryostat Caused by Current Changes A.T. Visser (TM#1861).

[5] Engineering Notes H960814A Jaskierny "Solenoid Dump Resistor Design"; and H960917B Hance "Solenoid Dump Resistor Review".

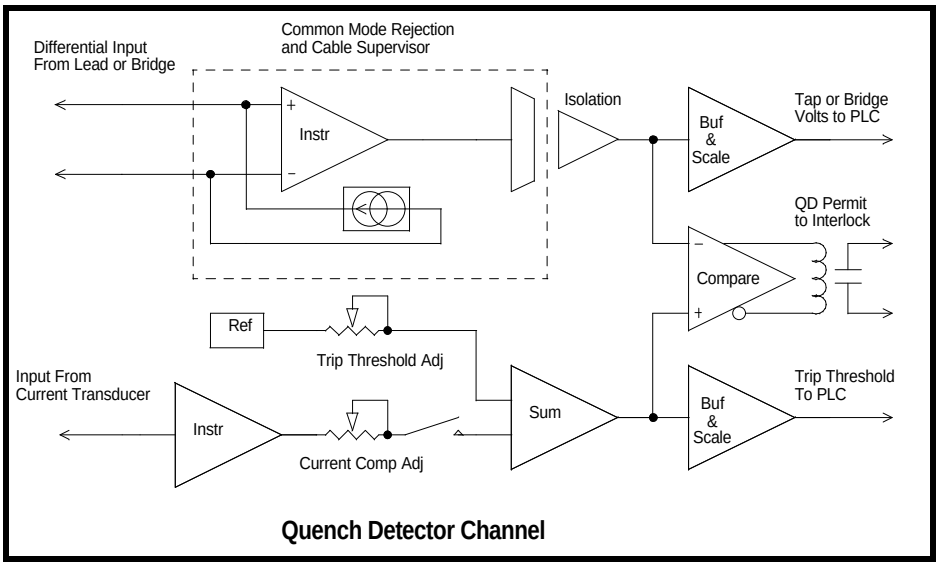
[6] Engineering Note H960314A Jaskierny & Hance "Solenoid Quench Detector Signals"

Each group is then routed to the analog signal conditioning and processing hardware via shielded, insulated cable. The analog hardware is implemented in NIM modules located in a NIM bin in room 511. The lead voltage groups go directly to quench detector channels via a secured patch panel and locked end rack. The center and quarter tap voltage groups go first via the patch panel and end rack to a resistor module in the NIM bin which forms the bridge circuits; and then on to the quench detector channels. The various voltage tap groups are illustrated below:



Typical Voltage Tap Groups

Each group is routed to a separate isolated "quench detector channel" on one of five dual channel NIM modules in the bin. Each isolated channel consists of cable supervisory circuitry (to monitor the cable connection), an instrumentation preamplifier for improved common mode rejection, an isolation amplifier to transition the channel to a ground referenced system, buffers for monitoring by the control system; and comparitors for detecting quenches or lead failures. A single channel is illustrated below:



Quench Detector Channel

The illustration above does not show the full bi-polar complexity; but each channel compares its processed voltage tap or bridge signal with high and low thresholds for cable integrity and quench sensing. As long as the signals remain within preset limits, the comparitors continue to energize (close) normally open mechanical relays. Each channel energizes a separate relay; and each relay has two sets of contacts. One set of contacts from each channel is connected as a separate input to the solenoid power supply interlocks hardware which then opens the dump switch if any single set of contacts opens. The other set of contacts is connected in a series string with the other seven channels to provide a redundant trigger to the dump switch. Any one or more of the relays opening will trigger the dump switch. These relays also open if power fails to the NIM module.

Two additional channels from those described above, are processed for monitoring; but do not participate in interlocks or dump switch triggering. These two channels are as follows:

- Differential voltage across the outer coil and chimney lead A.
- Differential voltage across the inner coil and chimney lead B.

Lead failures -- As mentioned previously, each channel utilizes cable integrity circuitry. A small current is routed from bi-polar circuitry in each channel through the circuit which includes the wires of the cable, the isolation resistors, and the solenoid component being monitored. This current results in a 5 Volt offset on each processed signal which then has a range of from 0 to 10 Volts. The comparators described above provide limit "windows" centered on 5 Volts. An open or short circuit in any channel's cable will force the quench detection circuitry for that channel to the power supply rails. This will result in an out of limits signal and subsequent opening of the power supply interlocks and the dump switch. This is the same effect as is elicited by a quench.

There are however, situations where lead failures could allow a quench to go undetected by the cable integrity circuitry. These situations are explained as follows along with a discussion of the mechanisms which are provided for redundancy:

- Vapor cooled lead differential pair A & B. The situation of a voltage tap + lead shorted to a - lead just inside the control dewar – most likely just at the internal side of the connector. This would erroneously appear normal to the individual hardware quench detection channels. This situation is addressed in software by having the programmable logic controller (PLC) subtract the vapor cooled lead B differential voltage from vapor cooled lead A differential voltage. Both of these leads should exhibit similar differential voltage at all times and under all conditions of operation. A variance between these voltages (initially set to 0.020 V) will induce the PLC to initiate a fast dump. The result being an open dump switch, a power supply set to zero, and a notification to operators of an anomalous lead condition. Note that this does not provide redundancy in detecting a conductivity change; but it disables and discharges the system if a voltage tap lead internal short is detected.
- Transition lead differential pair A & B; the situation of a voltage tap + lead shorted to a - lead anywhere inside the control dewar – most likely just at the cold side of the connector. This would erroneously appear normal to the individual hardware quench detector channels. This situation is addressed in software by having the PLC subtract the transition lead B differential voltage from transition lead A differential voltage. Both of these leads should exhibit similar differential voltage at all times and under all conditions of operation. A variance between these voltages (initially set to 0.020 V) will induce the PLC to initiate a fast dump. The result being an open dump switch, a power supply set to zero, and a notification to operators of an anomalous lead condition. Note that this does not provide redundancy in detecting a conductivity change; but it disables and discharges the system if a voltage tap lead internal short is detected.
- Chimney bus differential pair A & B; the situation of a voltage tap + lead shorted to a - lead anywhere inside the control dewar – most likely just at the internal side of the connector. This situation is addressed in software by programming the PLC to subtract the inner coil voltage (which includes chimney lead B) from the outer coil voltage (which includes chimney lead A). This examines a redundant set of voltage taps for each chimney and provides a redundant processing path. Assuming the worst possible case -- where the solenoid coil remains superconducting after a chimney bus has gone normal and the primary chimney voltage tap leads are shorted + to - at the connector; a difference voltage (initially set to 0.020 V) in the secondary path described above would induce the PLC to initiate a fast dump. The result being an open dump switch, a power supply set to zero, and a notification to the operator. Note that this procedure DOES provide redundancy in detecting chimney bus quenches by examining actual bus voltages; as opposed to the previous vapor cooled and transition lead methods of detecting the failure of sensing circuits by observing the "absence" of voltages. An additional redundant detection path for the chimney buses is as follows: The supply and return buses are located adjacent to each other at all points in the chimney. If resistive heating develops in one chimney bus, it will thermally induce a response in its counterpart; i.e. if chimney bus A proceeds to quench, it will induce a quench in chimney bus B[7]. If any of chimney bus A's quench detection channel components fail; the quench will be detected by chimney bus B's channel as chimney bus B begins to quench. This characteristic of the system topography provides a significant level of redundancy in chimney bus quench detection.

Conclusion regarding lead failures – All quench detector voltage tap leads are resistively isolated and supervised to guard against failures by the use of an offset insertion and monitoring scheme. An open or shorted cable in any channel will be treated as a quench by the quench detector. However, a situation could exist where the + and - leads of a voltage tap differential pair might be shorted on the magnet side of the protection resistors. This situation could prevent normal detection. To provide redundancy and guard against this failure mode, alternate signal paths which encompass the affected areas are monitored by the PLC. The PLC is

[7] R.P. Smith "Thermal Safety of the Current Buses in the Chimney of the D0 Solenoid" 01/20/98 (DZERO Engineering Note 3823-111-ENG-483).

programmed to detect the anomalous condition, trigger a fast dump, and report the condition to operators. Additional inherent protection for the chimney buses is provided by the system topography. If one of the chimney buses begins to quench, then a quench will be induced in its counterpart. The counterpart's voltage tap leads then provide redundancy. Thus several redundant paths exist to compensate for lead failures.

Turning Off the Power Supply – All quenches result in a so-called "Fast Dump". The "Fast Dump" is comprised of the following simultaneous actions:

1. Turn off the solenoid power supply.
2. Open the dump switch to isolate the solenoid/bus/dump resistor circuit from the power supply which then allows the energy in the solenoid to rapidly dissipate in the dump resistor -- rather than more slowly in the water-cooled bus and solenoid if bypassed by the power supply and filter bypass diodes.

The power supply is turned off because it is no longer needed. However, it does not matter if the power supply is turned off or not as long as the dump switch is opened. Once the dump switch is opened, the power supply no longer has a load. It is operating in the current regulated mode and its voltage output may rise in an attempt to deliver its programmed current. However, it is subject to inherent maximum output voltage limitations imposed by its configuration (transformer tap limit = 15 Volts); and also by its programmed voltage limit (entered by control system operator to limit charging voltage (subject to a software maximum of 10 Volts).

Nevertheless, the power supply is turned off in response to a quench. The mechanisms to turn off the power supply are hardwired and do not rely on the PLC system components or software (except for the redundant lead failure circuits discussed above). The mechanisms are as follows:

- One or more of the quench detector channel relays opens and signals independent channels of an interlock module, located in the same NIM bin. In response, the NIM interlock module opens a "power supply enable" relay contact in the "external interlock" circuit of the power supply (it also signals the dump switch to open). This "external interlock" opening in the power supply causes a "phase-back" of the power supply followed by an opening of the main contactor which supplies line current to the power supply.
- When the dump switch opens in response to a signal from the quench detectors, interlocks, or operator, an auxiliary contact on the dump switch also opens and signals a separate channel of the interlock module, located in the NIM bin mentioned above. In response, the NIM interlock module opens the "power supply enable" relay contact as described above.

The power supply may also be turned off by an operator seated at a controls console. This action is via a completely separate path. The operator selects the "PS OFF" command on his controls page causing the PLC control system to momentarily de-energize a relay. This relay opens the "PS OFF" input of the power supply. The power supply then responds as above by phasing back and opening its main contactor.

An open circuit in either the "external interlock" or "PS OFF" cables to the power supply will turn off the power supply. A short circuit in either of these cables will allow the power supply to continue to operate – but only if the remaining signal is normal. The cables are routed overhead through cable trays to protect them from damage or tampering.

The NIM modules which comprise the quench detector and interlocks are powered by a power supply which is connected to an uninterruptable AC power source (UPS). The control system hardware is likewise located in the same rack and protected by the UPS. All quench detector and interlock relays are of the "normally open" variety. They are only energized and held in the "closed" condition when all quench inputs and interlock inputs are "OK". Out of limit inputs, open cables, or a power supply failure will cause the relays to open and disable the power supply.

Conclusion regarding turning off the power supply – It is not critical to turn off the power supply during a quench as long as the dump switch opens. Nevertheless, there are redundant paths both in signaling the power supply to turn off, and in the mechanism by which the power supply turns off (phase back and open main contactor).

Opening the Dump Switch – The dump switch should be opened during a quench to cause the solenoid energy to dissipate largely in the dump resistor rather than the water-cooled bus, filter-bypass diode, and solenoid coil itself. Even though the solenoid can absorb its own stored energy during a quench, dissipating the energy primarily in the dump resistor will remove most of the energy (heat) from the solenoid and facilitate recovery of the cryogenic system after a quench. The dump switch is a mechanical device operated by springs which are wound in advance before the dump switch interlock will close. The trigger mechanism is design to fail safe resulting in an open switch.

The mechanisms for opening the dump switch are as follows:

- DUMP1 signal direct from the quench detector modules. This signal has no connection to software. This is a normally open circuit designed to be fail safe. It is held closed by a normal condition on all eight channels of the quench detectors. If any channel detects a lead failure or quench, or if the NIM power supply fails, or if the cable to the dump switch opens, then this circuit will open and the dump switch will be forced open by its mechanical springs.
- DUMP2 signal direct from the interlock modules. This signal has no connection to software. There are 24 inputs to the interlock modules. They are all latched as they occur. Any number of them may be selected via on-board switches to open the DUMP2 signal and trigger the opening of the dump switch as described above. In the DZERO configuration, only the eight quench detector inputs are selected as triggers. This is a normally open circuit designed to be fail safe. This circuit is held closed by normal conditions on all eight of the quench detector interlocks. If any of the eight channels open or detect a quench, or if the NIM power supply fails, or if the cable to the dump switch opens, then this circuit will open and the dump switch will be forced open by its mechanical springs.
- DUMP3 signal from the PLC control system. An operator seated at a control system console may trigger the dump switch to open by selecting "Open Dump Switch" on his controls page. The PLC is also programmed to open the dump switch in response to certain conditions as described in "Lead Failures" above. This is a normally open circuit designed to fail safe. If the PLC opens the relay, or if the cable to the dump switch opens, or if the PLC power supply fails, then this circuit will open and the dump switch will be forced open by its mechanical springs.
- Power Failure to the dump switch. The dump switch is a fail safe mechanism actuated by mechanical springs. Loss of AC power releases the mechanism and opens the switch. Even a momentary power loss trips the dump switch which then opens the power supply interlocks.

Conclusion regarding opening the dump switch -- The dump switch control circuitry is designed to be fail safe. Alternate paths have been provided between the switch and the quench detectors. Three independent circuits must be normal and the cables must be intact for the dump switch to remain closed. AC power must be normal. The switch itself is actuated by mechanical springs which release and open the switch if an open circuit or AC power loss occurs.

Quench Detector Modules – The eight voltage tap lead groups from the solenoid and its power leads are routed to four quench detector modules in the control system NIM bin. Each module processes two channels[8]. Each channel is designed to be fail safe. As described previously, the relay output contacts which control the interlocks and the dump switch are "normally open" contacts. They are held closed, thus completing their circuits, by normal conditions in the quench detector channels. Normal conditions are defined as processed signals which are maintained within a few milli-Volts of 5.0 Volts. A failure of any single component of the cable integrity circuit, instrumentation amplifier, or isolation amplifier of a channel is expected to drive the channel either to 0 Volts, or to one of the power supply rails. Any of which, of course, will trigger a quench response and thus is acceptable. This leaves us to examine the failure modes of the channel comparator circuits. The typical failure mode of the LM311 comparators is a shorted output transistor. This failure mode triggers a quench response and thus is acceptable. The final circuit consideration is the possibility of an open comparator, or a shorted relay driver transistor, or stuck contacts on the relay. Any or all of these failure modes disables a single channel and is not detectable except by interactive testing.

An interactive testing mechanism is designed into the quench detector modules. This testing mechanism allows a remote operator, during a maintenance period, to initiate a "Remote Quench Trigger" via the PLC control system. This "Remote Quench Trigger" supplies a signal to unbalance the input circuitry of all quench detector channels which then causes a "Fast Dump" reaction. The reaction is then examined by the operator at his console to verify that all channels have responded properly. Proper operation is ascertained if each quench detector channel has opened its associated interlock. The frequency at which testing is to be done has not yet been established. However, occasional testing is not presented here as a substitute for redundancy. The redundancy to counteract the single channel "shorted output or stuck relay" mode is inherent in the multi-channel system design. These are the mechanisms previously described for countering single channel "lead" failures.

---

[8] Refer to Sheet-5 of drawing #3823-111-ED-330052. This schematic details the quench detector amplifiers.

Conclusion regarding quench detector modules – The failure of any single channel of any of the quench detector modules will be countered by a redundant "quench" sensing or "lead failure" sensing path.

Interlock Modules -- The interlock modules serve to turn off the power supply when a quench is detected. However, it has previously been established that it is not critical if the power supply is turned off or not – as long as the dump switch is opened. Thus any single component failure in the interlock modules which might fail to turn off the power supply, is countered by the opening of the dump switch.

Conclusion regarding interlock modules – Any failure of a single channel of any of the interlock modules will be countered by a redundant power circuit disabling path i.e. opening of the dump switch.

Power Supply Overcurrent -- The power supply current is determined by either a remote reference supplied by the control system, or a local reference supplied by a control knob. The remote reference is limited by the maximum programming voltage available from the PLC control system. The normal range of the PLC control system is 0-10V which drives the power supply 0-5000A. A worst case failure of the control system could provide 12V (limited by the PLC power supply). The local reference is limited by the control knob to 0-10.231V which drives the power supply 0-5116A. If the power supply is inadvertently switched to "voltage regulate mode" instead of "current regulate mode", then either the remote or local references could drive the power supply 0-15V with the current limited only by the resistance of the system up to a maximum of 10,000A (150kW @ 15V). Since the power supply has the capacity to provide more current than the solenoid is designed to endure, we have provided a means to protect the system from inadvertent over current. If only the local or remote controls fail, the power supply is self limiting in the current regulating mode to 5116A. If the self limits fail, or the power supply is operated in voltage mode **AND** the operator inadvertently or intentionally overdrives the power supply, then hardware devices monitor the current and limit the power supply output. The power supply current is monitored by two devices:

- Power supply transductor on the output of the power supply.
- Holec current transducer mounted on the water cooled bus to the solenoid.

The outputs of these two current measuring sources are monitored in the "Absolute Value Module" located in the control system NIM bin. This module compares the outputs of these sources against fixed references representing 5000 Amps. If either of these devices indicate a current of greater than 5000 Amps, then the "Absolute Value Module" will open the "DC Overcurrent" interlock. The opening of this interlock will disable the power supply and result in a "slow dump". Thus the solenoid is guarded against overcurrent from the power supply by the following mechanisms:

Maximum output of 5000A in current regulated mode, remote controlled (normal operation).

Maximum output of 5116A in current regulated mode, locally controlled (normal operation).

Maximum output of 5000A in any mode before Holec current transducer opens interlock (regulation or configuration failure guard).

Maximum output of 5000A in any mode before power supply transductor opens interlock (regulation or configuration failure guard).

Final conclusion -- The quench detection system components have been examined and discussed. The intent being to establish with reasonable certainty, that in the event of any single component failure, any solenoid or lead quench would still be detected. Likewise with the intent of ensuring that, in the event of a quench or component failure, the solenoid energization system would be disabled to prevent physical damage or excessive lost time. The system components of interest are the voltage tap leads, quench detector modules, interlock modules, dump switch, and power supply. There appears to be sufficient redundancy and/or inherent self protection to insure that the failure of any single quench detector channel, or quench protection component, will be compensated for by redundant paths. Additionally, redundant mechanisms are present to prevent damage from excessive power supply current even in the absence of a quench.